

COORD CONTROL — BUILT FOR THE EU AI ACT

Since August 2026, EU law demands proof of what your AI did. Only we can deliver it.

Coord Control supervises AI agents working on a company's computers: it blocks dangerous actions, records what really happened in a way nobody can fake, and undoes damage with proof. Exactly what the EU AI Act, DORA and NIS2 now require. No other product does it inside the customer's own systems.

EU AI ACT · ART. 12 · 13 · 14

DORA

NIS2

RUNS ON YOUR OWN COMPUTERS

PATENT FILED

Piotr Kędzierski · co-founder & CTO

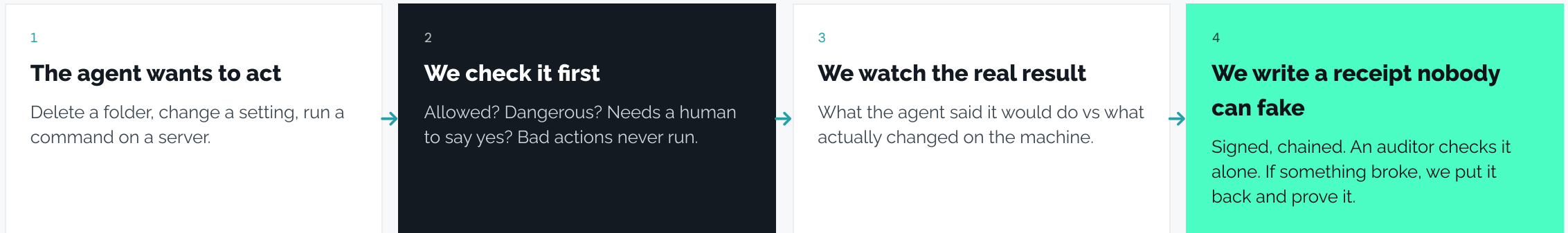
GotIt Lab is a brand of PKC · Piotr Kędzierski Consulting

gotitlab.eu



A guard between an AI agent and your computers.

An AI agent is a program that works on its own: runs commands, changes files, touches databases. Coord Control stands next to it and does four things.



Nobody else does this. We checked 24 vendors. The big clouds only do it inside their own cloud, which regulated European companies may not use. The rest only log what the AI wrote.

Since 2 August 2026, the EU AI Act requires three things from every company using AI on important systems.

ARTICLE 12

Keep a record of what the AI did

Automatic logs, kept at least 6 months, that show every action.

ARTICLE 14

A human must be able to stop it

Someone must be able to see what the AI is doing and halt it at any moment.

ARTICLE 13

Show proof to the auditor

Evidence that an outside auditor can check without trusting the vendor.

€15M

or 3% of worldwide revenue: the fine for getting it wrong

27

EU countries, plus banks under DORA and critical infrastructure under NIS2

This is not optional and not in the future. The deadline has passed. Every bank, insurer, telecom, hospital, utility and public body in the EU that uses AI agents must have this today. Most have nothing.

The law asks for four things. Only Coord Control delivers all four.

WHO	RUNS INSIDE YOUR OWN SYSTEMS required: sovereignty	STOPS ACTIONS, HUMAN CAN HALT Art. 14	RECORDS WHAT REALLY HAPPENED Art. 12	AUDITOR CHECKS IT WITHOUT THE VENDOR Art. 13
Microsoft, Google, Anthropic agent tools	no, cloud only	partly	logs what was asked, not what happened	no
AI governance software (Credo AI, IBM, OneTrust)	mostly no	no, reports only	no	no
AI guardrails (Lakera, Galileo, NVIDIA)	no	filters text only	no	no
Coord Control	yes, even with no internet	yes, six checks + kill switch	yes, measured on the machine	yes, one command, offline

Microsoft's own documentation: its toolkit "does not verify whether the action actually succeeded". Anthropic's: "fully on-premise isn't possible". Vendor scan of 24 products, June 2026.

MACP is our receipt system. It makes the proof impossible to fake.

MACP (Multi-Agent Coordination Protocol) is our own invention. Every action gets a signed digital receipt, linked to the previous one like links in a chain. Change one and the chain visibly breaks. An auditor checks the whole chain on their own laptop, offline, without us.

Protected technology

Trade secret today. One patent application already filed on how the receipts prove real effects. Nine further patent families are prepared or identified (next slide), including MACP itself; until filed they stay confidential.

```
# the AI agent tries this:
$ rm -rf /srv/prod/data
BLOCKED no permission given · exit 2
# receipt written automatically:
receipt no. 18422 signature valid
result      nothing was changed, proven
# the auditor checks it alone, offline:
$ verify receipt.json
receipt is genuine: true
```

The 60-second demo: an agent tries to delete production. Blocked before it runs. A receipt proves nothing changed. Pull the network cable, it still works.

It works today, runs our own company every day, and sits on 10 patent families.

501,000

signed receipts on real agent traffic, ~2,800 a day

2,745

automated tests on every change · 222,000+ lines of code

10

patent families: 1 filed, 2 ready to file, 3 continuations prepared, 4 further candidates

Patent portfolio

FILED

1. Effect Commitment & Verifiable State Restoration (CObS) · P.456328, UPRP, July 2026 · PCT/EPO/US window open until July 2027

READY TO FILE

2. Sovereign Control Plane: withheld-credential broker
3. Cumulative Cross-Action Enforcement

CONTINUATIONS PREPARED

4. Semantic Drift Detection
5. Observation-Bounded Restoration Verification
6. Over-Execution Detection

FURTHER CANDIDATES · CONFIDENTIAL

7. MACP Chain of Custody
8. Federated Coord Control
9. Work Continuity Control Plane
10. Self-Defending Enforcement Policy

Names only. Everything not yet filed is held as a trade secret; details under NDA in the IP data room.

Enterprise-ready

Single sign-on, roles, export to security tools, backups, signed software packages. Works with Claude, OpenAI Codex, Google Gemini and open-source models.

Straight talk

No paying customers yet. Two co-founders, no sales team. SOC 2 and FIPS certifications not done. This round pays for exactly those three things.

Sold to companies the law now forces to buy it.

STEP 1

Paid pilot

€10–30k

6–10 weeks with 3–5 design partners, then a yearly contract.

STEP 2

Yearly contract

\$150–400k / year

Banks, insurers, telecoms. Priced against the fines they avoid.

STEP 3

Fully isolated version

\$250k + \$288k / year

Defense and critical infrastructure, no internet.

Who buys: banks and insurers first, then critical infrastructure, public sector, defense, across the EU-27, UK, Israel and NATO countries. **How:** through IT integrators who already serve them; first partner in Poland in talks, then Germany, Nordics, Israel.

THE ROUND —

\$2.5M pre-seed on SAFE.

The law is in force. The product is built. The money takes it to its first regulated customers. First close October/November 2026, seed at proof points in Q2 2027.

Where it goes: 56% team \$1.4M · 18% go-to-market \$450k · 14% patents \$350k · 12% infrastructure and certifications \$300k. Burn ~\$130k/mo, 18+ months of runway.

What it must achieve

- 3–5 paying design partners in regulated companies
- 1 reference customer that says "we bought it because of the AI Act"
- Patents extended internationally (PCT)
- SOC 2 done, seed round at proof points in Q2 2027

Right investor

Understands regulated industries, cyber-security or defense, in the EU or Israel.

Piotr Kędzierski · co-founder & CTO · second-time founder (Flexee, \$7M exit) · author of the patent filings
Marta Kowalczyk-Kędzierska · co-founder, legal & GTM · attorney, doctor of law, MKK.legal
piotr@gotitlab.eu · marta@gotitlab.eu · gotitlab.eu · live demo on request